SUSTAINABLE MACHINE INTELLIGENCE JOURNAL

SFMR-SH: Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare Using Blockchain Technology

Jamal A Alenizi[1], and Ibrahim Alrashdi[2,*]

[1] Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka 2014, Saudi Arabia; 431100002@ju.edu.sa.
[2] Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka 2014, Saudi Arabia; irrashdi@ju.edu.sa.
* Correspondence: irrashdi@ju.edu.sa.

Abstract: As the healthcare industry increasingly relies on digital technology and the Internet of Things (IoT) to improve patient care and streamline operations, the vulnerability to ransomware attacks has become a significant concern. In response to this pressing issue, we present SFMR-SH (Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare), a groundbreaking approach that integrates IoT devices with blockchain technology to fortify healthcare data security. SFMR-SH leverages blockchain's inherent properties, including immutability and transparency, to create an impervious fortress for sensitive patient data. Through comprehensive simulations employing machine learning algorithms (KNN, SVM, Random Forest, Gradient Boosting, and XGB), we assess the framework's ability to detect and mitigate ransomware attacks. Results underscore the framework's effectiveness, achieving an impressive detection accuracy of 99.33%. This research represents a significant stride in fortifying smart healthcare systems, providing a secure environment amid the escalating threat landscape, and ensuring the uninterrupted delivery of vital healthcare services. Our findings highlight the exceptional promise of SFMR-SH in revolutionizing healthcare data security, safeguarding patient privacy, and fortifying the future of smart healthcare systems in an increasingly digitalized healthcare landscape.

Event	Date
Received	03-01-2023
Revised	18-03-2023
Accepted	26-03-2023
Published	27-03-2023

Keywords: Smart Healthcare, Ransomware Attacks, Blockchain Technology, Data Security, Cybersecurity, Machine Learning, Digital Health Services, Internet of Things (IoT), Medical IoT Devices, Patient Privacy, Cyber Threats.

1. Introduction

The Internet of Medical Things (IoMT) is a subset of the Internet of Things (IoT) that focuses on remote patient monitoring, examination, and treatment through telehealth services. With the rapid proliferation of smart IoMT devices worldwide, especially following the COVID-19 pandemic, healthcare faces unprecedented challenges. By 2025, global expenditures on healthcare technology are projected to reach $135 billion. However, the widespread adoption of IoMT devices and the healthcare system's reliance on them have raised significant concerns about data safety and security. Securing the data collected, transmitted, and stored by IoMT systems is paramount. Unlike other data systems, IoMT systems directly impact patients' lives and can breach their privacy if sensitive information is exposed. Notably, healthcare data is fifty times more valuable than credit card data, underscoring the fundamental need for robust security measures. Despite its significance, the resource-intensive nature of IoMT systems, along with inherent limitations, makes them susceptible to various threats [4].

Recent studies highlight the security risks faced by smart healthcare systems. Vulnerabilities in hospital infrastructure can grant attackers unauthorized access to critical data, jeopardizing the integrity of medical facilities. This vulnerability presents a severe threat, particularly when considering the potential exploitation of sensitive information in ransomware attacks. Unprotected medical devices are at risk of malware attacks that enable unauthorized access to medical records, posing a substantial risk of data loss [3]. The increasing frequency of these breaches underscores the high likelihood of ransomware attacks targeting the healthcare sector. The emergence of Blockchain technology in recent years has revolutionized data security practices. Blockchain operates as a decentralized model for data processing, ensuring the immutability, validity, and transparency of all transactions between network nodes [4]. Its capacity to efficiently provide operational, verification, and regulatory services positions Blockchain as a promising solution to the security challenges faced by the healthcare industry.

The rapid evolution of cloud services and the proliferation of diverse IoT devices within smart healthcare settings have given rise to heightened concerns regarding data protection and security. The sensitive nature of healthcare data makes it an attractive target for cyberattacks, and the increasing deployment of IoT devices with inadequate security measures exacerbates this vulnerability. While fog nodes facilitate edge processing within the network, a pressing issue remains the absence of robust security solutions at these nodes. Ransomware attacks have emerged as a prominent threat to smart healthcare systems, underscoring the urgent need for comprehensive security measures to detect and mitigate such attacks. This revised problem statement succinctly encapsulates the key challenges and emphasizes the importance of addressing ransomware attacks in smart healthcare systems. It sets a clear direction for your research work. If you have any further questions or require assistance with other sections of your paper, please feel free to ask.

In light of these developments and the pressing need to safeguard smart healthcare systems, this study outlines its research objectives.

- **Identify Vulnerabilities in Smart Healthcare Systems:** Conduct a comprehensive analysis to identify vulnerabilities within smart healthcare systems, including patient data, medical records, and operational infrastructure. Explore potential entry points for ransomware attacks, considering factors such as social engineering, phishing, and system vulnerabilities.
- **Analyze Ransomware Threats:** Investigate various ransomware threats targeting smart healthcare systems, examining their modes of entry, encryption techniques, and methods of extortion. Understand the evolving landscape of ransomware attacks in healthcare, with a focus on tactics employed by attackers to exploit system weaknesses.
- **Evaluate Blockchain Technology in Healthcare:** Assess the potential of blockchain technology in enhancing the security and efficiency of smart healthcare systems. Explore

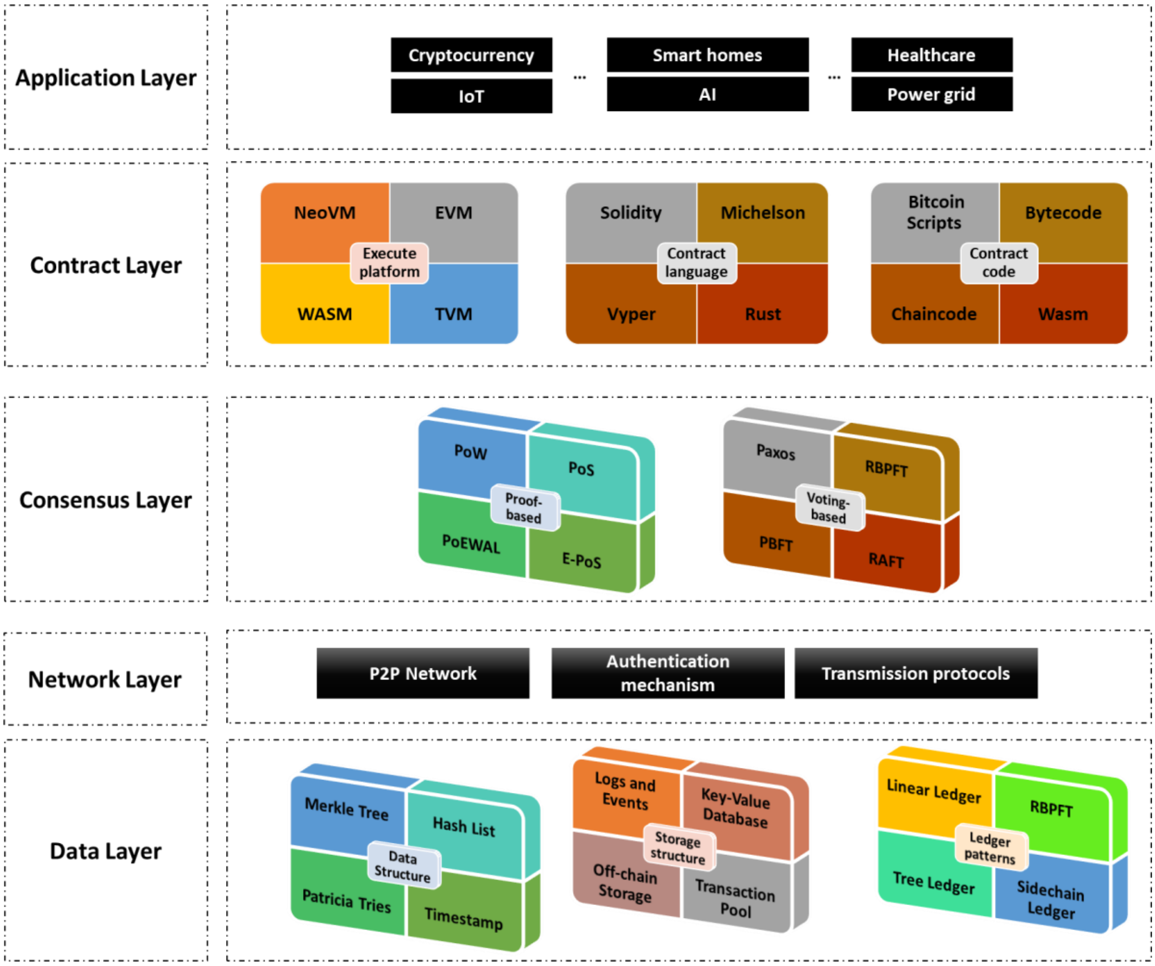

Figure 1. Blockchain architecture

how blockchain can address challenges related to data storage, management, and integrity within healthcare settings. Analyze the feasibility of integrating blockchain solutions into existing healthcare infrastructures.

- **Develop a Secure Framework:** Design and develop a robust security framework leveraging blockchain technology to mitigate ransomware attacks in smart healthcare systems. Focus on creating a comprehensive defense mechanism that addresses identified vulnerabilities and offers real-time threat detection, prevention, and response capabilities. Ensure the framework's adaptability and scalability to cater to diverse healthcare environments.
- **Validate and Optimize the Framework:** Implement the developed framework in a simulated smart healthcare environment to validate its effectiveness. Conduct rigorous testing and optimization to ensure the framework's reliability, accuracy, and efficiency in detecting and mitigating ransomware attacks. Gather empirical evidence to support the framework's practical applicability and potential for real-world implementation.

This research holds a significant place in the realm of smart healthcare system security, addressing the pressing issue of an increasing number of threats faced by healthcare systems daily. The growing concerns about the security of smart healthcare systems underscore the importance of conducting comprehensive studies to enhance their efficiency and fortify defenses against potential attackers. With the advent of the IoMT, there are new opportunities for researchers to identify vulnerabilities and develop effective solutions to safeguard these systems.

Research Contributions:

This research makes several substantial contributions that advance the field:

- Firstly, it conducts a thorough review of the latest research in the domain of securing smart healthcare systems, with a particular emphasis on countering electronic threats, notably ransomware.
- Secondly, it delves into a detailed investigation of numerous risks and vulnerabilities that could impact the seamless functioning of blockchain-based smart healthcare systems.
- Furthermore, it introduces a novel and robust framework specifically designed to mitigate the growing threat of healthcare ransomware attacks. The performance of this framework within the context of smart healthcare is critically analyzed.
- Lastly, this research provides valuable insights by comparing the proposed framework with existing solutions and similar outcomes, highlighting the cost-effectiveness of the newly proposed approach in terms of computational efficiency and communication overhead.

The remaining sections of this research paper are structured as follows: In Section 2, we conduct a comprehensive examination of ransomware attacks and elucidate the essential security requirements to combat them effectively. Section 3 provides a summary of various related approaches. Moving to Section 4, we embark on a detailed exploration of the various phases comprising the proposed blockchain-enabled framework for mitigating ransomware attacks in smart healthcare systems. Section 5 is dedicated to a rigorous security analysis of the framework, scrutinizing its resilience against potential threats and vulnerabilities. In Section 6, we concludes the research, summarizing the key findings.

2. Background

In this section, we embark on a comprehensive exploration of ransomware attacks within the context of smart healthcare systems. our aim is to elucidate the multifaceted nature of these attacks, dissect their methods of entry and operation, and highlight the security requirements necessary to mount a robust defense against them.

3. Blockchain Technology in Healthcare

In the healthcare industry, the infrastructure supporting applications and managing crucial data, including electronic health records (EHRs), contains highly sensitive assets. These records encompass personal data such as names, addresses, social security numbers, and medical histories, necessitating the utmost security and confidentiality. Unfortunately, cyberattacks have targeted this treasure trove of personal information, resulting in the theft of millions of patient records from various medical organizations [6]. Blockchain, often referred to as BC, offers a distributed ledger system of irreversible transactions. Nodes in the network maintain a ledger by executing transactions within blocks, which are verified through a consensus process and linked by cryptographic hashes, creating an immutable chain of records that propagates through a peer-to-peer consensus network [1]. The security of blockchain transactions predominantly relies on their secure execution. In healthcare, blockchain technology is employed to grant patients access to vital records while preserving their privacy. Ensuring secure data exchange is imperative to prevent unauthorized access and exploitation of sensitive medical information. The permanence and immutability of blockchain technology are intrinsic strengths, as it cryptographically secures records within a chain of blocks, rendering them unalterable [16]. Blockchain offers several advantages, including:

Decentralization: Decision-making occurs without the need for central authority.
Transparency: Every action is documented, and users maintain access to immutable data records.
Reliability: Trust is established through the consensus of multiple, often unfamiliar participants.
Consistency: Transactions become immutable and indestructible when connected to the blockchain.
Processing Efficiency: The adoption of blockchain has significantly reduced startup and processing times, from days to minutes or seconds [28].

The potential benefits of blockchain in healthcare are exemplified by the collaboration between the US Food and Drug Administration (FDA) and IBM Watson Health, which developed a blockchain framework to safeguard oncology-related data. This technology enables the collection of data from diverse sources, securely storing it in a transaction audit log, and facilitating accounts receivable tracking. Blockchain's ability to reduce the likelihood of catastrophic breaches, ensure data integrity, anonymity, and resilient storage, as well as minimize single points of failure, becomes evident in such applications [29]. Blockchain technology, unlike existing centralized cloud computing architectures, enables collaboration among unknown and untrusted entities while supporting the distributed nature of mobile devices in smart health. It is built upon an immutable "public ledger," a shared record of data among all participants. Data blocks are linked through cryptographic hash keys, and consensus-based linking methods such as Proof of Work (PoW) ensure data integrity. This architecture resists data alteration, as modifying block data would invalidate earlier block hashes, disrupting consensus among nodes (refer to Figure 1). Blockchain technology allows secure and cost-effective digital currency transactions without relying on a third party for authentication, mitigating the "double spending" problem. Each transaction initiates the execution of a smart contract, offering decentralized control, data transparency, auditability, distributed information, and protection from malicious actors [29].

4. Ransomware attack

Ransomware is a pervasive threat in the digital landscape, with two primary variants garnering particular attention: crypto and locker ransomware. Notably, threat actors have evolved their tactics, venturing into the realms of double extortion and Ransomware as a Service (RaaS), elevating the menace they pose. Locker Ransomware: One prominent strain

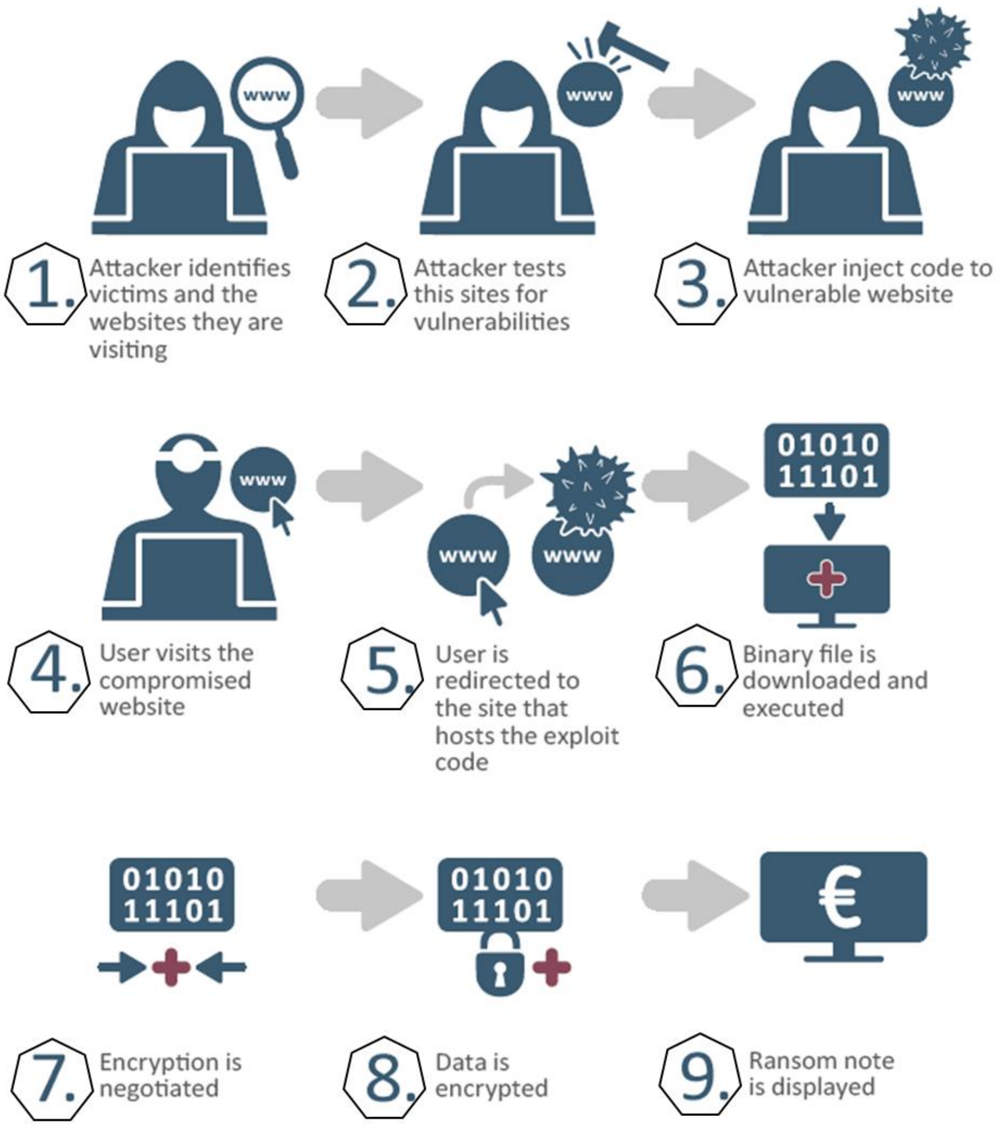

Figure 2. Ransomware attack on smart healthcare systems

of ransomware, known as locker ransomware, effectively denies users access to their own computers. This insidious program employs stolen credentials and social engineering techniques to infiltrate systems. Once inside, threat actors lock out users and demand a ransom to restore access. Victims may encounter alarming pop-up messages on their screens, asserting that their computer has been involved in illicit activities and necessitates a hefty fine for rectification (refer to Figure 2).

Crypto Ransomware: In contrast, crypto ransomware, a more prevalent and widespread form, encrypts files on a computer or network. It then demands a ransom in exchange for the decryption key required to regain access to the compromised files. Recent iterations of crypto ransomware have extended their reach to infect networked, cloud, and shared storage. These malicious programs commonly spread through downloads, fraudulent websites, and malicious emails. Double Extortion Ransomware: An emerging and concerning trend among ransomware variants is double extortion ransomware. This

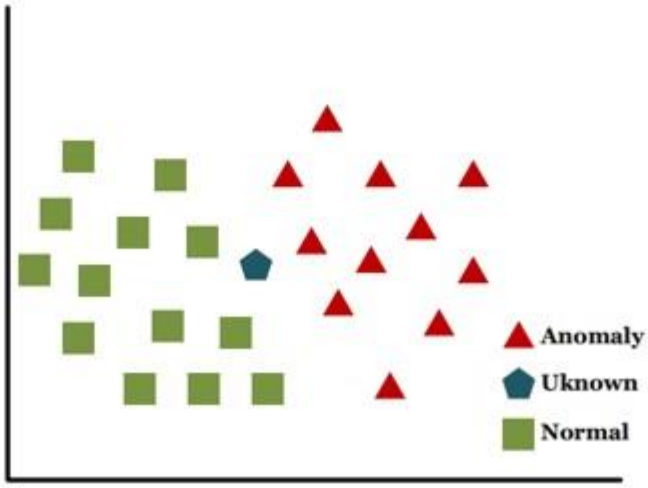

Figure 3. K-Nearest Neighbor (KNN) classification principle

category combines file encryption with data exfiltration. In essence, attackers not only encrypt victims' files but also extract sensitive data. This dual threat coerces victims into paying the ransom by intertwining data recovery with the possibility of exposing stolen information. Even if victims recover their data from backups, the attacker retains leverage through the stolen data.

Ransomware as a Service (RaaS): The landscape of ransomware has further evolved with the advent of Ransomware as a Service (RaaS). In this model, ransomware developers offer specific ransomware strains as a pay-per-use service to criminals. RaaS vendors operate on the dark web, mirroring the "software as a service (SaaS)" model, where criminals subscribe to these services. After successfully infecting devices, subscribers are obligated to remit a portion of their illicit gains to the RaaS authors. Several notorious ransomware attacks have left their mark on the cybersecurity landscape, including Locky, WannaCry, Bad Rabbit, Ryuk, Shade/Troldesh, Jigsaw, CryptoLocker, Petya, and GoldenEye [17]. These ransomware strains have collectively highlighted the multifaceted nature of the ransomware threat, underscoring the imperative for robust countermeasures and heightened cybersecurity vigilance.

5. Machine Learning

Machine learning (ML), a subset of artificial intelligence (AI), represents a technology that harnesses computational data to emulate intelligent behaviors with minimal human intervention. The journey of AI, which finds its roots in the world of robotics, has accelerated with advancements in electronic speeds and programming, paving the way for computers to mimic human-like intelligence. In the realm of computer science, this endeavor is termed artificial intelligence, where machines autonomously simulate intelligent behavior, often relying on machine learning techniques [20].

K-Nearest Neighbors (KNN): KNN, a versatile classification algorithm, distinguishes itself by requiring no initial parameters. The metric of choice to measure distances between neighbors is typically the Euclidean distance. The core concept underlying KNN involves

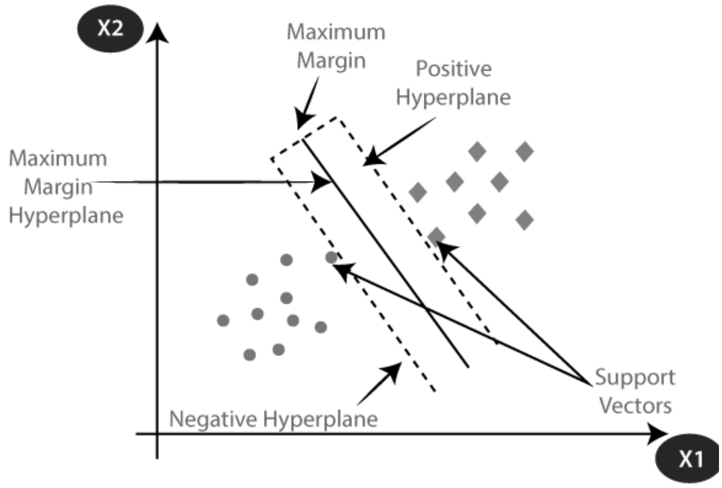

Figure 4. Support Vector Machine (SVM) classification principle

categorizing incoming data instances into previously observed classes based on their proximity to each class (refer to Figure 3). In essence, any newly observed, unknown instance is classified by considering its nearest neighbors from known classes. The parameter 'K' signifies the approximate number of neighbors employed in the classification process [21].

Support Vector Machine (SVM): Support Vector Machine (SVM), a popular supervised learning algorithm, finds applications in solving classification and regression problems, with a predominant focus on classification. SVM's objective revolves around establishing an optimal decision boundary, often referred to as a hyperplane, capable of dividing n-dimensional space into distinct classes (refer to Figure 4). This decision boundary facilitates the rapid classification of new data points. Key to SVM's operation are the support vectors, representing extreme instances that influence the construction of the hyperplane [29].

XGBoost Algorithm: XGBoost, short for Extreme Gradient Boosting, represents a scalable machine learning system for tree boosting. This technique, known as boosting, is employed in both classification and regression problems. Boosting involves iteratively constructing weak learners, with each step contributing a new one to the overall model. XGBoost stands out in its application of gradient direction, derived from the loss function, to build these weak learners (refer to Figure 5). It distinguishes itself from Random Forest

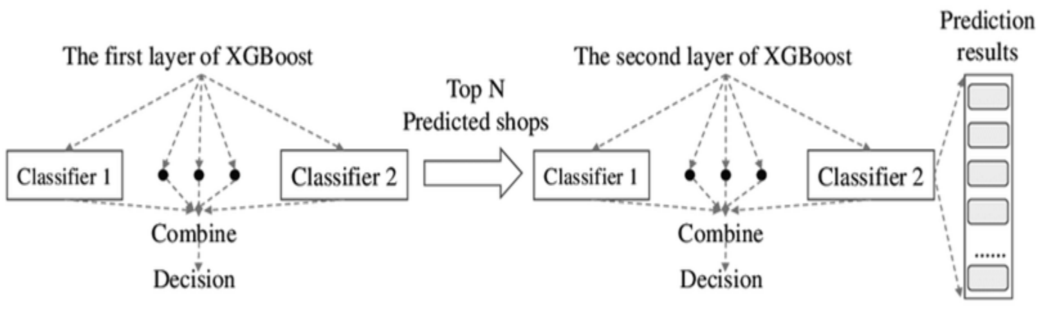

Figure 5. XGBoosting model

(RF) in that GBM (Gradient Boosting Machines) adds new trees to enhance existing ones, while RF builds independent trees [25].

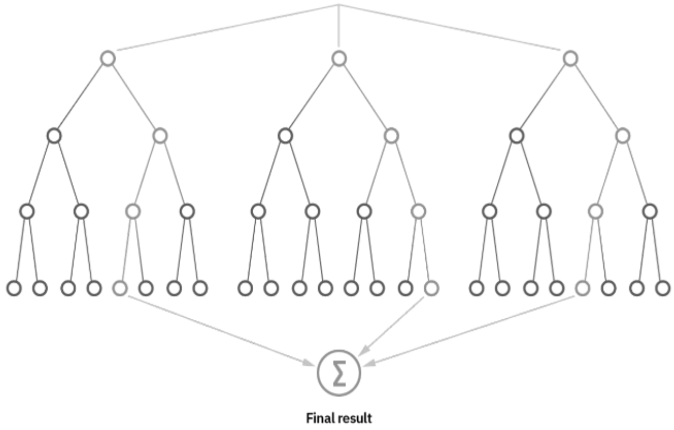

Figure 6. Random Forest model

Random Forest (RF): RF stands as a well-reputed and effective ensemble supervised classification method. Its versatility extends to various machine learning applications, including bioinformatics and medical imaging, owing to its superior accuracy and robustness. RF is particularly adept at providing insights through feature ranking. This ensemble method consists of decision trees, generated through the bagging algorithm without pruning. The result is a "forest" of classifiers, collectively contributing to class prediction (refer to Figure 6). RF requires two primary parameters: the number of trees in the forest (ntree) and the number of randomly selected features evaluated at each tree node (mtry), along with a training database featuring ground-truth class labels [26].

6. Related work

Recent advancements in the field of smart healthcare security have ushered in a surge of studies dedicated to understanding and mitigating the vulnerabilities and threats that pose challenges to the optimal functioning of smart healthcare systems. Numerous studies, as exemplified by references [2, 14, 24], have centered on the perils of vulnerabilities and threats, where cybercriminals exploit these weak points. Such attacks, including ransomware incursions, have highlighted the complexities of managing and safeguarding healthcare data. These attacks underscore the urgent need to secure healthcare records and protect patient lives. Blockchain technology has emerged as a compelling solution to address these challenges, primarily due to its capacity for privacy, security, strict constraints, and ecosystem-wide interoperability. Patient data security takes center stage in several pivotal studies, as evidenced by references [1, 5, 13]. Patient data, laden with sensitive information, engenders concerns and anxieties among individuals. It becomes imperative to reevaluate protective and privacy measures surrounding this sensitive information. This entails a meticulous examination of data storage mechanisms, treatment processes, storage space, and backup protocols to avert potential threats such as data loss and corruption. Recent ransomware attacks, notably during the COVID-19 pandemic, have underscored the vulnerability of healthcare providers, leaving countless individuals without access to essential medical services.

The increased adoption of smart healthcare systems, a phenomenon elucidated in research [3, 4, 6], stems from the allure of remote healthcare services, which mitigate the need for physical visits to healthcare facilities. These systems facilitate the management of Electronic Health Records (EHRs) containing a wealth of personal and sensitive data. These records encompass names, addresses, social security numbers, insurance details, and medical histories. This trove of personal information holds immense value for patients, healthcare providers, insurers, and research institutions. However, the prevalence of cyberattacks on smart healthcare systems poses a significant challenge. Creating, issuing, and maintaining medical certificates can be plagued by problems like forgery, jeopardizing privacy and documentation. Blockchain technology stands as a promising avenue for processing smart healthcare operations efficiently and securely. Nevertheless, complex vulnerabilities in blockchain technology persist, hindering healthcare data transactions, particularly in the face of ransomware attacks.

References [7, 15, 22] have presented comprehensive reviews of smart healthcare security frameworks, applications, challenges, and future research directions. As healthcare systems transition from traditional to modern smart healthcare setups, characterized by the integration of emerging technologies like the Internet of Things (IoMT), big data analytics, and artificial intelligence, vulnerabilities of these devices to ransomware attacks loom large. These attacks not only imperil patient data but also inflict substantial damage. Cybercriminals invest considerable effort, time, and resources into the exploitation and monetization of healthcare data. The sheer volume of healthcare data, reaching approximately 2,314 exabytes in 2020, underscores the magnitude of the challenge. Blockchain technology, combined with machine learning and software-defined networks, emerges as a potent tool for real-time detection and prevention of ransomware attacks during clinical trials and beyond.

Further studies, as denoted by references [18, 19, 22], emphasize the criticality of securing data from loss and damage during creation and cloud storage. In the face of escalating cyberattacks, the imperative for detection processes employing machine learning techniques gains prominence. Utilizing IPFS and Blockchain technology to fortify medical material and record storage emerges as a potent strategy. Blockchain, recognized as a secure and trustworthy platform for information exchange across diverse domains including healthcare, fosters fast, seamless, and secure interactions, thereby enhancing privacy and data security.

Table 1. Comparison of previous research

			Study areas					Software			
Study	**Year**	**Issues Discussed**	**Confidentiality**	**privacy**	**Access control**	**Data storge**	**vulnerabilities**	**Yes**	**No**	**Advantages**	**Limitations**
[1]	2022	Blockchain as a potential tool to mitigate the impacts and difficulties of fog computing		√				√		Blockchain can overcome the	The lack of comparison between the current methods

										privacy of fog computing	and the suggested solution.
[2]	2022	Various open issues and challenges of smart healthcare systems.					√	√		Risk is evaluated by different performance metrics in blockchain	Vulnerable to Ransomware Attacks
[3]	2021	Interface between users and healthcare centers to generate and maintain health documents.			√				√	An improvement in efficiency over previous schemes	the lack of empirical evaluation of the system's security.
[4]	2023	Reduce transaction delays and processing costs while detecting a ransomware attack					√	√		Reduces transaction delays of 4-10 minutes and processing costs by 10% for healthcare data compared to the previous one	Cost High Computation
[5]	2022	Build a secure, real-time, and tamper-proof monitoring of medical data		√			√	√		An acceptable improvement to the privacy of medical data	It need to Re-Examine
[6]	2021	Evaluate the security standards that underpin blockchain technology	√	√	√			√		Significant improvement on security, regulatory compliance, compatibility, flexibility, and scalability	Cost High Computation
[12]	2023	Storing healthcare data on hospital blockchain networks		√		√			√	Improve efficiency and adaptability.	Cost High Computation
[13]	2023	Detecting smart healthcare ransomware attacks		√		√	√			Achieving better accuracy than previous verses	Cost High Computation
In this research	2023	Securing smart healthcare systems from the risks of cyber-attacks, especially ransomware.	√	√	√	√	√	√			The study will cover all the previous gaps

7. Proposed Framework: SFMR-SH

In this section, we delve into the heart of our proposed solution, the Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare, or SFMR-SH. SFMR-SH represents a comprehensive and innovative approach to addressing the growing concerns surrounding cybersecurity in the realm of smart healthcare systems. As smart healthcare continues to advance and transform the way medical information is generated, stored, and shared, it has become increasingly vulnerable to ransomware attacks and other malicious cyber threats. SFMR-SH is designed to safeguard the integrity and privacy of sensitive medical data by leveraging the power of blockchain technology and machine learning. This section will provide a detailed exploration of the four pivotal steps within SFMR-SH, shedding light on the creation of healthcare data backups through blockchain, the application of machine learning for ransomware detection and analysis, the mitigation of ransomware attacks, and the recovery of data through blockchain transactions.

7.1. Data Backup Creation via Blockchain

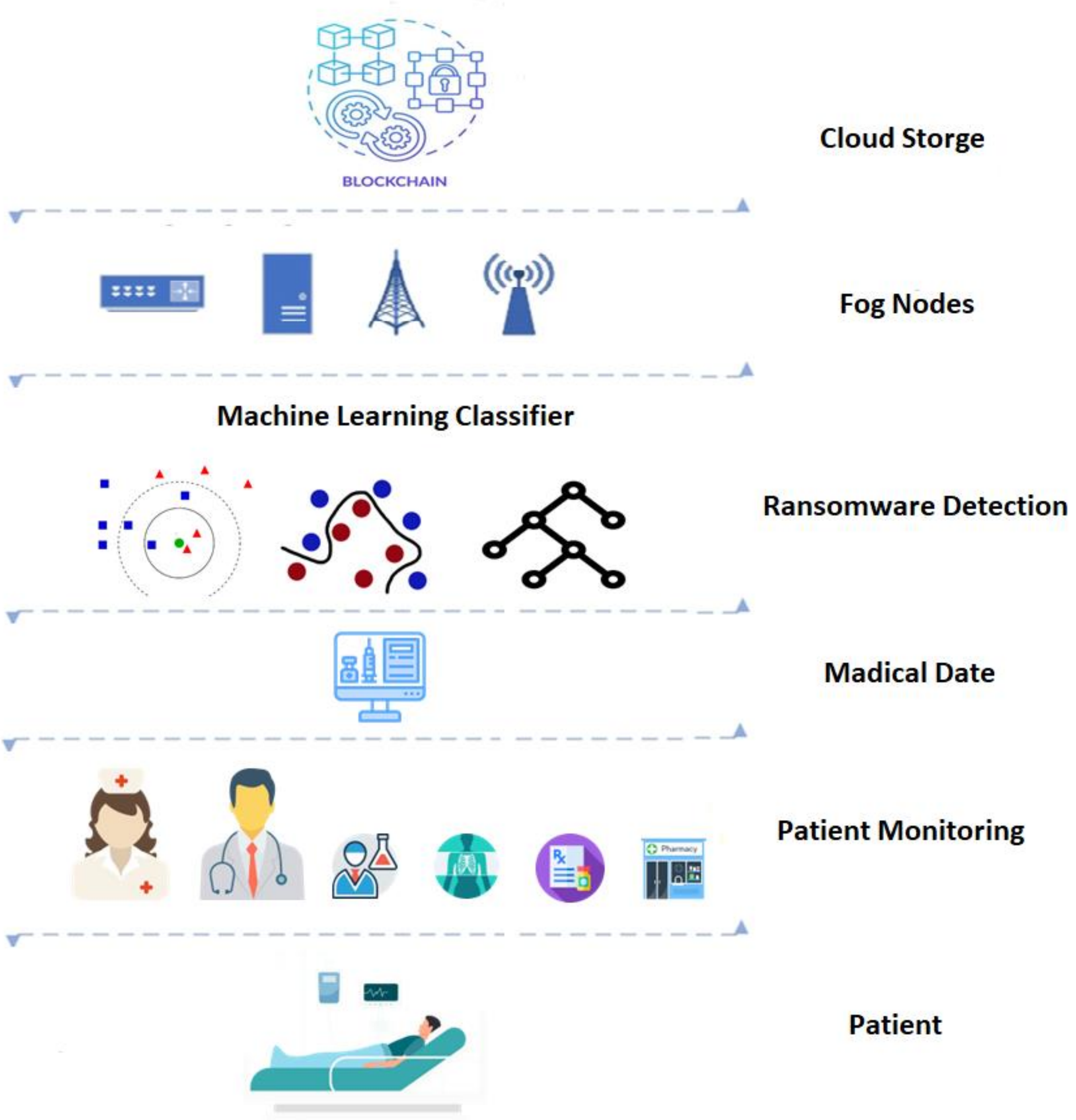

Figure 7. Overview of medical data transaction creation over a blockchain

Smart medical data generation relies on Internet of Medical Things (IoMT) devices, seamlessly connected to the human body. These devices record vital signs, such as heartbeats, alongside essential medical data like x-rays and lab results. The recorded data, collected through sensors, is meticulously monitored by medical professionals, including doctors and nurses, who manage medications, medical records, and reports. Following thorough processing and verification, the data is transmitted to the examination center for ransomware attack screening. If the data is deemed secure, it is subsequently stored in cloud storage via fog nodes. (Refer to Figure 7 for an overview of the medical data transaction creation process over a blockchain.)

7.2. Ransomware Detection and Analysis Using Machine Learning (ML)

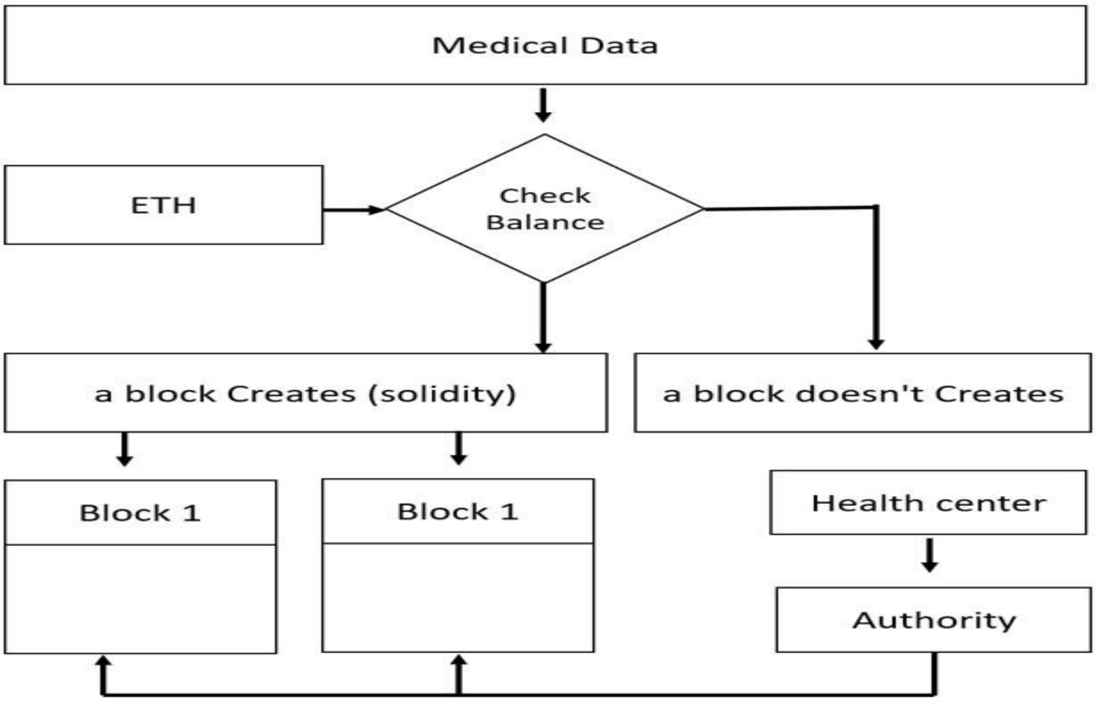

Figure 8. Medical data transaction creation over a blockchain

In the processing phase, the medical data undergoes scrutiny at the ransomware attack screening unit. Employing machine learning tools, this unit ensures the integrity of the medical data. Suspicious data, indicating a potential ransomware attack, is isolated and withheld from transmission to the fog nodes. Conversely, if the data passes the ransomware scrutiny, it proceeds to the fog nodes. To validate the efficacy of SFMR-SH in detecting ransomware, a dataset from Kaggle [32] was employed, and machine learning algorithms (KNN, SVM, XGB, Random Forest) were assessed. The dataset encompasses various features related to the heterogeneous Bitcoin network, designed for identifying ransomware payments. It comprises multivariate, time-series data with 2,916,697 instances and ten attributes, including Bitcoin address, year, day, length, weight, count, looped, neighbors, income, and label (categorized as ransomware family or benign). This evaluation necessitated using 90% attackers (ransomware) and 10% benign samples, albeit with potential implications for false positive rates (FPR) [13].

7.3. Ransomware Mitigation and Control

SFMR-SH incorporates mechanisms to mitigate the impact of ransomware, employing machine learning techniques for identifying and classifying the extent of ransomware's spread. When anomalies indicative of ransomware are detected, the proposed method swiftly isolates compromised medical equipment or systems, thereby preventing the further proliferation of ransomware. This proactive approach significantly enhances security by identifying and countering malicious viruses like WannaCry, PowerGhost, and Petya, which pose severe security threats to smart healthcare data (refer to Figure 8).

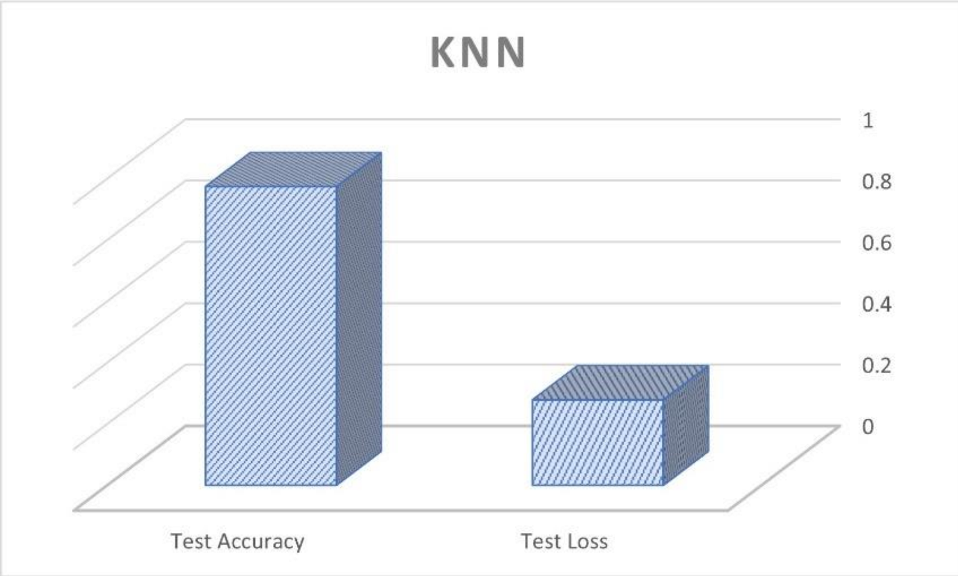

Figure 9. Ransomware attack detection by KNN

7.4. Data Retrieval and Blockchain Transactions

The data recovery phase involves several key components and actions:

- **Solidity:** A programming language used to write code lines that facilitate actions on the blockchain when creating a smart contract.
- **ETH (Ethereum):** A balance denoting the cryptocurrency used for transaction financing within the blockchain, often managed through wallets like MetaMask.
- **Block:** Patient information is stored on the blockchain as a transaction within a specific block.
- **Check Balance:** Information is only recorded as a transaction in the block when there is sufficient balance.

8. Results and Discussion

In this section, we present the results of our Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare (SFMR-SH) and delve into their implications and insights. SFMR-SH is designed to integrate Internet of Things (IoMT) devices with a blockchain-based storage system, offering a holistic approach to enhance healthcare data security while reducing the risks associated with ransomware attacks.

Figure 11. Ransomware attack detection by XGB

The core of SFMR-SH's success lies in its utilization of blockchain technology, which inherently brings several advanced properties to the table. Firstly, the immutability of blockchain ensures that once healthcare data is recorded, it becomes tamper-proof, preventing unauthorized alterations or deletions. Transparency is another significant benefit, as every transaction is recorded in the blockchain, creating an audit trail that enhances accountability and trust.

Our evaluation demonstrates that SFMR-SH effectively reduces the rate of ransomware attacks on healthcare data. This reduction is primarily attributed to the machine learning techniques employed to analyze data traffic. Machine learning plays a pivotal role in identifying patterns and anomalies indicative of ransomware activities. The integration of fog computing further enhances data processing and storage efficiency before transmitting it to the cloud, resulting in a more robust defense against ransomware threats.

Importantly, SFMR-SH is a globally applicable model that allows authorized users to access smart healthcare systems in real-time. The unique Blockchain Transaction Identifier (BCT_ID) assigned to patient data enables secure access from anywhere, at any time, contributing to improved patient care and accessibility. The performance of blockchain technology in our framework is noteworthy. It significantly reduces transaction delays and lowers processing costs for healthcare functions, both on cloud and mobile cloud nodes. This efficiency is particularly critical in the context of healthcare, where timely access to patient data can be a matter of life and death (refer to Figure 9-12).

Machine learning's role in SFMR-SH cannot be overstated. It simplifies healthcare system management, aiding in predicting ransomware attacks and detecting anomalous

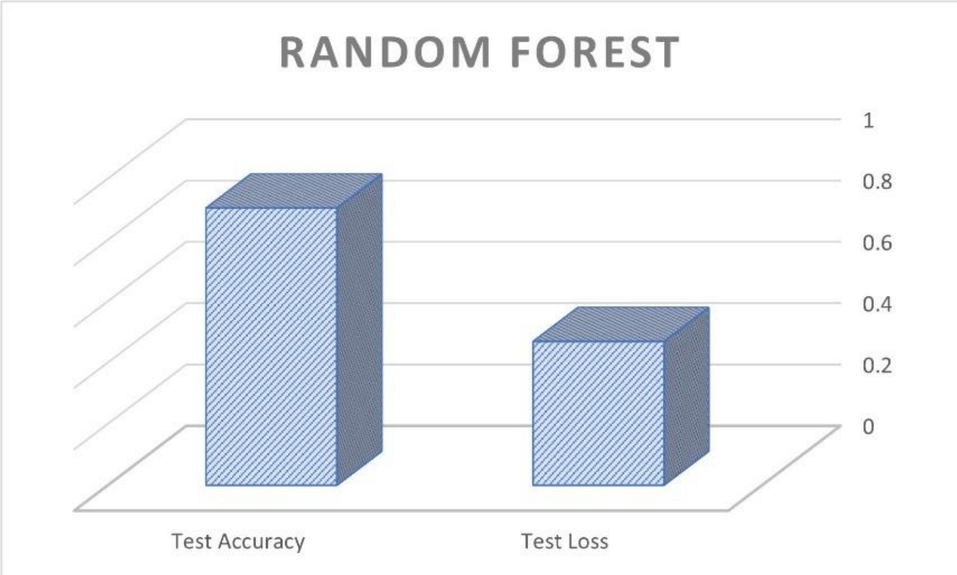

Figure 12. Ransomware attack detection by Random Forest

network behaviors. Given the increasingly sophisticated nature of cyber threats, the integration of machine learning is crucial for staying ahead of attackers.

Comparing SFMR-SH with previous studies underscores its exceptional ability to detect and mitigate attacks using machine learning algorithms. In particular, the Support Vector Machine (SVM) learning algorithm demonstrated outstanding performance with a detection accuracy score of 99.03%. This achievement signifies a significant advancement in healthcare data security (refer to Figure 13).

Furthermore, our blockchain security framework has proven effective in detecting and mitigating ransomware attacks. The low accuracy and loss rates observed during simulations indicate the framework's potential to reduce the risks associated with ransomware attacks in the healthcare sector. These results are encouraging and highlight the promise of SFMR-SH in safeguarding patient data.

9. Conclusions

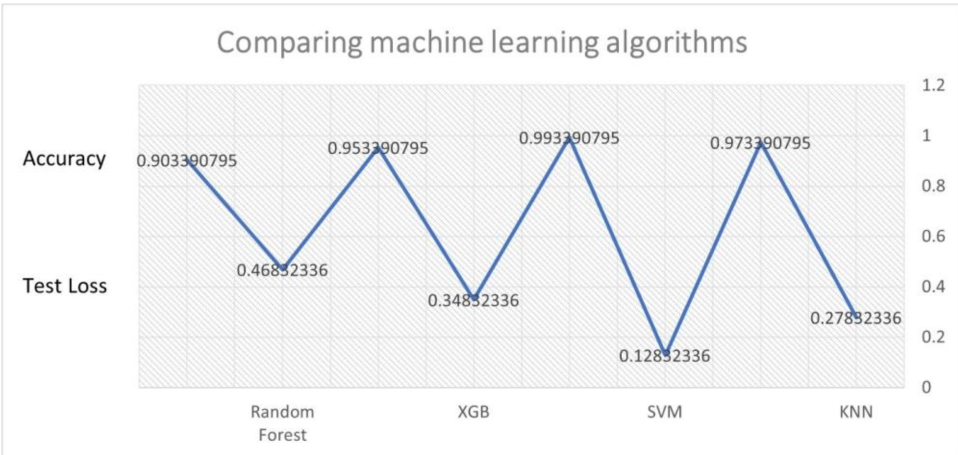

Figure 13. Comparison of ransomware attack detection by learning algorithms

In this study, we have presented SFMR-SH (Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare), an innovative approach that integrates Internet of Things (IoMT) devices with blockchain-based storage systems to enhance healthcare data security and combat the rising threat of ransomware attacks in the healthcare sector. Our research demonstrates the effectiveness of SFMR-SH in leveraging blockchain's advanced properties, such as immutability and transparency, to create a tamper-proof environment for patient data. Through the integration of machine learning techniques, we have successfully reduced the rate of ransomware attacks and improved the efficiency of healthcare data processing and storage. SFMR-SH offers a globally applicable model, ensuring real-time access to smart healthcare systems for authorized end-users, thus enhancing patient care and accessibility. The outstanding performance of machine learning algorithms, particularly the Support Vector Machine (SVM), underscores SFMR-SH's potential to revolutionize healthcare data security. As ransomware attacks continue to evolve in sophistication, SFMR-SH stands as a robust defense mechanism, offering insights into the vital role of blockchain technology and machine learning in safeguarding patient data. This work marks a significant step towards securing the future of smart healthcare systems and preserving patient privacy in an increasingly digital healthcare landscape.

Supplementary Materials

Not applicable.

Author Contributions

For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, J.A. and I.A.; methodology, J.A.; software, I.A.; validation, J.A., and I.A.; formal analysis, J.A.; investigation, I.A.; resources, I.A.; data curation, J.A.; writing—original draft preparation, I.A.; writing—review and editing, J.A.; visualization, I.A.; project administration, I.A. All authors have read and agreed to the published version of the manuscript.

Funding

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Data Availability Statement

All data generated or analyzed during this study are included in this article.

References

[1]. Alam, S., Shuaib, M., Ahmad, S., Jayakody, D. N. K., Muthanna, A., Bharany, S., & Elgendy, I. A. (2022). Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration. Sustainability, 14(22), 15312.

[2]. Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. Applied Sciences, 12(21), 11039.
[3]. Namasudra, S., Sharma, P., Crespo, R. G., & Shanmuganathan, V. (2022). Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. IEEE Consumer Electronics Magazine, 12(2), 83-93.
[4]. Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International journal of advanced research in computer science*, *8*(5), 1938-1940.
[5]. Ch, R., Srivastava, G., Nagasree, Y. L. V., Ponugumati, A., & Ramachandran, S. (2022). Robust cyber-physical system enabled smart healthcare unit using blockchain technology. Electronics, 11(19), 3070.
[6]. Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M. H., & Kerrache, C. A. (2021). The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications, 2(1), 100012.
[7]. Wazid, M., Das, A. K., Mohd, N., & Park, Y. (2022). Healthcare 5.0 security framework: applications, issues and future research directions. IEEE Access.
[8]. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.
[9]. Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications*, *190*, 116198.
[10]. Maigida, A. M., Abdulhamid, S. I. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. Journal of Reliable Intelligent Environments, 5, 67-89.
[11]. Maigida, A. M., Abdulhamid, S. I. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. Journal of Reliable Intelligent Environments, 5, 67-89.
[12]. Mukati, A. Blockchain Technology In Healthcare Services.
[13]. Wazid, M., Das, A. K., & Shetty, S. (2022). BSFR-SH: Blockchain-enabled security framework against ransomware attacks for Smart Healthcare. IEEE Transactions on Consumer Electronics, 69(1), 18-28.
[14]. Thamer, N., & Alubady, R. (2021, April). A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 210-216). IEEE.
[15]. Tariq, U., Ullah, I., Yousuf Uddin, M., & Kwon, S. J. (2022). An Effective Self-Configurable Ransomware Prevention Technique for IoMT. Sensors, 22(21), 8516.
[16]. Thamer, N., & Alubady, R. (2021, April). A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 210-216). IEEE.
[17]. Namasudra, S., Sharma, P., Crespo, R. G., & Shanmuganathan, V. (2022). Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. IEEE Consumer Electronics Magazine, 12(2), 83-93.
[18]. Liu, H., Crespo, R. G., & Martínez, O. S. (2020, July). Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. In Healthcare (Vol. 8, No. 3, p. 243). MDPI.
[19]. Zakaria, W. Z., Abdollah, M. F., Mohd, O., Yassin, S. W. M. S. M., & Ariffin, A. (2022). RENTAKA: A Novel Machine Learning Framework for Crypto-Ransomware Pre-encryption Detection. International Journal of Advanced Computer Science and Applications, 13(5).
[20]. Battineni, G., Sagaro, G. G., Chinatalapudi, N., & Amenta, F. (2020). Applications of machine learning predictive models in the chronic disease diagnosis. Journal of personalized medicine, 10(2), 21.
[21]. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics, 9(7), 1177.
[22]. Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. Security and Privacy, 4(5), e162.
[23]. Dorogush, A. V., Ershov, V., & Gulin, A. (2018). CatBoost: gradient boosting with categorical features support. arXiv preprint arXiv:1810.11363.
[24]. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70-83.
[25]. Pan, B. (2018, February). Application of XGBoost algorithm in hourly PM2. 5 concentration prediction. In IOP conference series: earth and environmental science (Vol. 113, p. 012127). IOP publishing.
[26]. Petkovic, D., Altman, R., Wong, M., & Vigil, A. (2018). Improving the explainability of Random Forest classifier–user centered approach. In Pacific symposium on biocomputing 2018: proceedings of the pacific symposium (pp. 204-215).
[27]. Quasim, M. T., Algarni, F., Radwan, A. A. E., & Alshmrani, G. M. M. (2020, July). A blockchain based secured healthcare framework. In 2020 International Conference on Computational Performance Evaluation (ComPE) (pp. 386-391). IEEE.
[28]. [Online]. Available:Support Vector Machine (SVM) Algorithm - Javatpoint
[29]. Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: a survey. Procedia Computer Science, 175, 615-620.

[30]. Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, *11*(10), 1198.
[31]. Thamer, N., & Alubady, R. (2021, April). A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)* (pp. 210-216). IEEE.
[32]. [Online]. BitcoinHeistRansomwareAddressDataset (kaggle.com)